REMARKS

In the Office Action, the Examiner indicated that claims 1 through 21 are pending in the application and the Examiner rejected all claims.

Claim Objections

On page 2 of the Office Action, the Examiner objected to claims 2, 3, 9, 10, 16, 17 and 19 due to various informalities. Each claim has been amended as suggested by the Examiner. In light of these amendments, the Examiner is respectfully requested to reconsider and withdraw the objections to claims 2, 3, 9, 10, 16, 17 and 19.

Claim Rejections, 35 U.S.C. § 101

On page 3 of the Office Action, the Examiner rejected claims 8-14 under 35 U.S.C. §101 as being directed to non-statutory subject matter. In response, Applicants have amended claim 8 to include a plurality of agents, which are defined as tangible hardware interfaces in the specification. In light of this amendment, the Examiner is respectfully requested to reconsider and withdraw the rejections of claims 8-14 under 35 U.S.C. §101.

Claim Rejections, 35 U.S.C. §§ 102 and 103

On page 4 of the Office Action, the Examiner rejected independent claims 1, 8 and 15 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0233581 to Reshef et al. ("Reshef").

On page 5 of the Office Action, the Examiner rejected claims 2, 9 and 16 under 35 U.S.C. §103(a) as being unpatentable over Reshef in view of Applicants' admitted prior art (AAPA).

On page 6 of the Office Action, the Examiner rejected claim 3-5, 10-12 and 17-20 under 35 U.S.C. §103(a) as being unpatentable over Reshef in view of U.S. Patent Application Publication No. 2004/0064722 to Neeley et al. ("Neeley").

On page 9 of the Office Action, the Examiner rejected claims 7, 14 and 21 under 35 U.S.C. §103(a) as being unpatentable over Reshef in view of U.S. Patent Application Publication 2003/0236994 to Cedar et al. ("Cedar").

The Present Invention

The present invention teaches a method and system for the automatic detection and correction of security vulnerabilities in both individual software components and across complex, multi-component software solutions. The present invention utilizes a plurality of vulnerability analysis and fortification tool (VAF) agents to analyze and proactively identify possible ways to attack a software component. Both legal (e.g., a registered user) and illegal (e.g., an unregistered user) interfaces are examined for vulnerabilities . Specifically, claim 1 recites "analyzing by a plurality of agents a software solution to identify legal and illegal external interfaces thereto" (lines 3-4). Once any illegal interfaces are identified, the interfaces are used to attempt to illegally access the software component. Claim 1 further recites "attempting to access said software solution using the identified illegal external interfaces" (lines 5-6). Once the access attempts are completed, any resulting information is stored in a record at a series of databases

associated with the VAF agents. Claim additionally recites "storing a record of any illegal external interfaces that allow access to said software solution at a plurality of databases associated with said plurality of agents" (lines 7-8).

U.S. Patent Application Publication No. 2003/0233581 to Reshef et al.

U.S. Patent Application Publication No. 2003/0233581 to Reshef et al. ("Reshef") teaches a method for detecting security vulnerabilities in a web application includes analyzing the client requests and server responses resulting therefrom in order to discover pre-defined elements of the application's interface with external clients and the attributes of these elements. The client requests are then mutated based on a pre-defined set of mutation rules to thereby generate exploits unique to the application. The web application is attacked using the exploits and the results of the attack are evaluated for anomalous application activity.

U.S. Patent Application Publication No. 2004/0064722 to Neeley et al.

U.S. Patent Application Publication No. 2004/0064722 to Neeley et al. ("Neeley") teaches executing a vaccine program on a computer, where the program searches for a known vulnerability in software on the computer. Upon detecting a vulnerability, the program triggers execution of code that performs at least one non-malicious activity to effect reducing risk associated with the vulnerability, such as generating a notification or applying a software patch to neutralize the vulnerability.

U.S. Patent Application Publication No. 2003/0236994 to Cedar et al.

U.S. Patent Application Publication No. 2003/0236994 to Cedar et al. ("Cedar") teaches a master test engine for accessing a primary manifest data file which describes verification tests to be performed by each of a set of computers to be tested. To execute the tests within the primary manifest data file, one or more test executables are created. The text executables are run by local test engines which are located on each one of the computers on which tests are conducted.

The Cited Prior Art Does Not Anticipate the Claimed Invention

The MPEP and case law provide the following definition of anticipation for the purposes of 35 U.S.C. §102:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP §2131 citing *Verdegaal Bros. v. Union Oil Company of California*, 814 F.2d 628, 631, 2 U.S.P.Q. 2d 1051, 1053 (Fed. Cir. 1987)

The Examiner Has Not Established a *Prima Facie* Case of Anticipation

As noted above, the present claimed invention includes a plurality of agents for analyzing a software solution to identify legal and illegal interfaces to the software, and using the illegal interfaces to test the security of the software. Having a plurality of agents running the test is beneficial as it allows unique testing at a variety of sites over a distributed computer network. For example, a single software application maybe distributed across 20 networked computers. Each computer, however, has a different set of illegal interfaces and only by having an individualized

agent for analysis and testing will each of the illegal interfaces be identified and analyzed. This differs from the prior art, including Reshef.

Reshef teaches a method for detecting security vulnerabilities in a web application running on a single web server. Incoming client requests for the server are analyzed and mutated to create possible problems and then submitted to the server. The results are analyzed and the security for the server is increased based upon the results of the submission. This is useful in monitoring and protecting a single web server, but it is not the same as the present invention. The present invention claims a plurality of agents used to analyze and test software in a distributed computing environment. This is in direct contrast with the invention of Reshef, which has only a single web server and no distributed computing. Without a teaching of a plurality of agents analyzing software, Reshef cannot anticipate the present invention. As such, each of the independent claims (claims 1, 8 and 15), and all claims depending therefrom, patentably define over Reshef and are in condition for allowance.

The Examiner Has Not Established a *Prima Facie* Case of Obviousness

As set forth in the MPEP:

> To establish a *prima facie* case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skilled in the art, to modify the reference or to combine reference teachings.
> MPEP 2143

As discussed above, Reshef fails to teach a plurality of agents analyzing legal and illegal interfaces to a computer solution. The addition of either Neeley or Cedar, as suggested by the Examiner, still fails to teach or reasonably suggest the presently claimed invention.

Neeley teaches a vaccine program on a computer, where the program searches for a known vulnerability in software on the computer. However, the vaccine of Neeley is for use on a local computer only and has no teaching of using a plurality of agents for analyzing legal and illegal interfaces. As such, the combination of Reshef in view of Neeley fails to teach or reasonably suggest the present invention.

Similarly, Cedar teaches a master test engine for creating a set of tests to be executed on a computer. However, this master test engine runs on a single server (similar to Reshef), and no teaching of a plurality of agents is present in Cedar. As such, the combination of Reshef in view of Cedar fails to teach or reasonably suggest the present invention.

In light of the foregoing arguments, the Examiner is respectfully requested to reconsider and withdraw the rejections of claims 3-5, 10-12 and 17-20 under 35 U.S.C. §103(a) as being unpatentable over Reshef in view of Neeley. Similarly, the Examiner is respectfully requested to reconsider and withdraw the rejection of claims 7, 14 and 21 under 35 U.S.C. §103(a) as being unpatentable over Reshef in view of Cedar.

Conclusion

The present invention is not taught or suggested by the prior art. Accordingly, the Examiner is respectfully requested to reconsider and withdraw the rejection of the claims. An early Notice of Allowance is earnestly solicited.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment associated with this communication to Deposit Account No. 19-5425.

Respectfully submitted,

November 20, 2007
Date

/John R. Brancolini/
John R. Brancolini
Registration No. 57,218

SYNNESTVEDT & LECHNER LLP
1101 Market Street
Suite 2600
Philadelphia, PA 19107

Telephone: (215) 923-4466
Facsimile: (215) 923-2189

S:\I\IBM\IBM RALEIGH RSW\PATENTS\P27239 USA\PTO\REPLYTOOA08222007.DOC